An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2504110151

NCSC Advisory

Critical Vulnerability in Windows Common Log File System (CLFS)

CVE-2025-29824

11th, April 2025

STATUS: TLP:CLEAR

Description

CVE ID: CVE-2025-29824

Published: 2025-04-08

Vendor: Microsoft

Product: The vulnerability impacts multiple Windows versions. For the full list of affected products, please see table below.

CVSS Score[1]**:** 7.8

Products Affected

Product	Version
Windows 10 Version 1809	10.0.17763.0 < 10.0.17763.7137
Windows Server 2019	10.0.17763.0 < 10.0.17763.7137
Windows Server 2019 (Server Core installation)	10.0.17763.0 < 10.0.17763.7137
Windows Server 2022	10.0.20348.0 < 10.0.20348.3454
Windows 10 Version 21H2	10.0.19043.0 < 10.0.19044.5737
Windows 11 version 22H2	10.0.22621.0 < 10.0.22621.5191
Windows 10 Version 22H2	10.0.19045.0 < 10.0.19045.5737
Windows Server 2025 (Server Core installation)	10.0.26100.0 < 10.0.26100.3775
Windows 11 version 22H3	10.0.22631.0 < 10.0.22621.5191
Windows 11 Version 23H2	10.0.22631.0 < 10.0.22631.5191
Windows Server 2022, 23H2 Edition (Server Core installation)	10.0.25398.0 < 10.0.25398.1551
Windows 11 Version 24H2	10.0.26100.0 < 10.0.26100.3775
Windows Server 2025	10.0.26100.0 < 10.0.26100.3775
Windows 10 Version 1507	10.0.10240.0 < 10.0.10240.20978
Windows 10 Version 1607	10.0.14393.0 < 10.0.14393.7970

[1] https://www.first.org/cvss/

Windows Server 2016	10.0.14393.0 < 10.0.14393.7970
Windows Server 2016 (Server Core installation)	10.0.14393.0 < 10.0.14393.7970
Windows Server 2008 Service Pack 2	6.0.6003.0 < 6.0.6003.23220
Windows Server 2008 Service Pack 2 (Server Core installation)	6.0.6003.0 < 6.0.6003.23220
Windows Server 2008 Service Pack 2	6.0.6003.0 < 6.0.6003.23220
Windows Server 2008 R2 Service Pack 1	6.1.7601.0 < 6.1.7601.27670
Windows Server 2008 R2 Service Pack 1 (Server Core installation)	6.1.7601.0 < 6.1.7601.27670
Windows Server 2012	6.2.9200.0 < 6.2.9200.25423
Windows Server 2012 (Server Core installation)	6.2.9200.0 < 6.2.9200.25423
Windows Server 2012 R2	6.3.9600.0 < 6.3.9600.22523
Windows Server 2012 R2 (Server Core installation)	6.3.9600.0 < 6.3.9600.22523

Impact

Use after free in Windows Common Log File System Driver (CLFS) allows an authorised attacker to elevate privileges locally.

Microsoft have identified a threat actor group leveraging this flaw through the PipeMagic malware to gain SYSTEM-level access to perform post-exploitation activities such as credential dumping via LSASS and deploying ransomware.

Common Weakness Enumeration (CWE)[2]: CWE-416: Use After Free

Known Exploited Vulnerability (KEV) catalog[3]: Yes

Used by Ransomware Operators: Yes

[2] https://cwe.mitre.org

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Microsoft.

- https://nvd.nist.gov/vuln/detail/CVE-2025-29824
- https://www.cve.org/CVERecord?id=CVE-2025-29824
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-29824
- https://www.microsoft.com/en-us/security/blog/2025/04/08/exploitation-of-clfs-zero-day-leads-to-ransomware-activity/